COMPARISON OF TECHNIQUES FOR ASSESSING NUCLEAR POWER PLANT PROTECTION AGAINST SABOTAGE AND HIGH LEVEL WASTE (HLW) REPOSITORY PROTECTION AGAINST HUMAN INTRUSION

Steven E. Mays
ACRS/ACNW Fellow

April 1991

ABSTRACT

Human actions have the potential to bypass the protective features that minimize the likelihood of release of radioactive material to the environment from nuclear power plants or a geologic high level waste (HLW) repository. Sabotage of nuclear power plants and human intrusion into a geologic repository are examples of acts of commission that the NRC and EPA respectively have concluded require specific regulations. This paper compares the use of probabilistic techniques by the two agencies in dealing with these acts of commission. The NRC chose a deterministic approach for assessing the impact of sabotage on power plants and limited the use of probabilistic techniques to qualitative assessments of the adequacy of licensee security plans. EPA chose to require treatment of human intrusion quantitatively as an explicit part of the performance assessment required for licensing a geologic HLW repository.

COMPARISON OF TECHNIQUES FOR ASSESSING NUCLEAR POWER PLANT PROTECTION AGAINST SABOTAGE AND HIGH LEVEL WASTE (HLW) REPOSITORY PROTECTION AGAINST HUMAN INTRUSION

INTRODUCTION

Nuclear power plants have engineered features and proposed HLW repositories have engineered and geologic features that serve to limit the likelihood of release of radioactive material to the environment. In the case of nuclear power plants, several engineered barriers exist including the fuel cladding, the reactor coolant system boundary, and the containment. For spent fuel at a nuclear plant, the barriers include the fuel cladding and the spent fuel pool (or dry cask storage at some locations). For a HLW repository the proposed barriers include the fuel cladding, the containers for the spent fuel, and the geological formation (analogous to the reactor containment).

Human actions such as sabotage or human intrusion have the potential to bypass the features that limit the likelihood of release of radioactive material to the environment. While the intent of the participants and the nature of these two actions are different, such events are difficult to analyze by probabilistic techniques and at least sabotage is not so treated. This paper examines the extent that the two agencies use probabilistic techniques to regulate protection from these acts of commission. It is not intended to equate the physical acts themselves nor to state that the approach suggested here is the final word on the subject.

The NRC and EPA have regulations[1,2] requiring licensees to demonstrate their ability to maintain the integrity of the features against certain acts of commission. In the case of nuclear power plants, physical security requirements for protection against sabotage are contained in 10 CFR 73.55. For a HLW repository, the EPA requirements for human intrusion (HI) are contained in an appendix to 40 CFR 191.

While both agencies recognize the potential for human actions to bypass these protective features, the use of probabilistic techniques in the licensing and regulatory process is vastly different. Briefly stated, the EPA regulations require a quantitative probabilistic analysis (called a performance assessment) of the performance of the protective features of a repository over a 10,000 year period. This assessment must include human intrusion scenarios explicitly. The NRC approach with respect to sabotage at nuclear power plants, on the other hand, eschews quantitative probabilistic criteria in favor of a deterministic evaluation supported by qualitative use of probabilistic analyses.

The purpose of this paper is to compare the methods used by the NRC and EPA to regulate protection from sabotage at reactors and inadvertent human intrusion at a potential HLW repository. The paper specifically addresses the use of (or the lack of) probabilistic techniques in their regulations and applications. While there may be concerns regarding the similarity of the events themselves (and therefore the applicability of comparing the types of regulation) and

whether either agency has come upon the ultimate methodology for regulating them, this paper compares the regulations and applications as they currently exist. It is for the reader to determine the applicability of these techniques to the regulation of protection against sabotage at reactors and human intrusion at a HLW repository.

PROBABILISTIC TECHNIQUES

In any discussion of probabilistic analysis, definitions are important. Since the terms used by the two agencies differ somewhat, it is necessary to define the terms in this paper with respect to the two agency's terms.

The EPA regulations require, as a licensing condition for a HLW repository, a "performance assessment" of any potential site. The EPA has set release limits for various radionuclides and constructed a probabilistic criteria that the performance assessment needs to satisfy. Specifically, the assessment must analyze a variety of scenarios that could result in release of radioactive material to the environment and calculate a complementary cumulative distribution function (CCDF) that shows the likelihood of releases to be below the EPA's probabilistic limits. In nuclear power plant probabilistic risk assessment language, this is known as a "risk curve". This paper will use the terms CCDF and risk curve synonymously.

For nuclear power plants, risk curves are a quantitative part of the process known as probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA). Thus, the performance assessment of the EPA requirements is analogous to a PRA for a nuclear plant. The elements of a PRA needed to generate a risk curve are a set of initiating events, a model of the plant response to these events (event trees and fault trees), and a model of the consequences of the various sequences derived from the models. Figure 1 shows the three major elements of a PRA along with its equivalent element from a performance assessment required by the EPA. The PRA risk curve is generated by propagating data distributions for the initiating events, plant response models, and consequence models to arrive at a distribution for each of the undesired sequences in the models. A distribution is derived for the sum of the sequence distributions and the risk curve (CCDF) for the result is produced. The equivalent elements of an EPA performance assessment are scenario development, HLW containment behavior models, and transport models. Distributions are propagated through these mathematical models in a manner similar to the PRA methods (although the mathematical models for containment and transport are much different from the event/fault tree models of PRA). The combination of the resulting distributions is used to produce the CCDF for comparison to the EPA requirements.

SABOTAGE VERSUS HUMAN INTRUSION

As noted before, both the NRC and the EPA recognized the potential for human actions to adversely impact the protective features of a nuclear power plant or potential HLW repository. The method for dealing with these two similar issues is vastly different.

Human actions that adversely impact the performance of protective features are

generally characterized by the PRA community as either acts of omission or acts of commission[3,4]. Acts of omission are cases where a required action does not occur. Acts of commission are cases where actions occur that adversely impact the protective features in spite of the fact that the action is neither required nor desired.

This paper characterizes sabotage and human intrusion as examples of acts of commission. While the intent of the participants in both cases is drastically different as is the physical nature of the actions, probabilistic analysis of acts of commission is the same. Current PRA practice excludes acts of commission from the quantitative process due to the inability to calculate either the frequency of such acts or their effects on the protective features. This paper compares the NRC use of probabilistic analysis techniques for regulating protection from sabotage to the EPA requirements for probabilistic analysis of human intrusion for a geological repository. It is not intended to equate the actions themselves.

NRC Approach to Sabotage

The NRC chose a deterministic, rather than a quantitative probabilistic approach, for dealing with sabotage. In fact, even with the current maturity of PRA (as compared with the emerging performance assessment techniques), the NRC has not used a risk curve as a licensing criteria for any plant, much less for the subset of events that would include sabotage.

The NRC approach recognized the inherent uncertainties and lack of data for quantifying the nature of or the probability of a sabotage event. It also recognized the difficulty in assessing the damage a potential sabotage event would have on the operation of the engineered features for limiting the release of radioactive material. In other words, quantifying sabotage initiating events and their effects on plant systems was impractical.

The NRC conducted studies to assess the threat level that plants would be required to address in their security plans. Their rules[1,5,6] recognized that a graded approach to sabotage protection at nuclear power plants (in comparison with nuclear weapons facilities or weapons grade material facilities) was appropriate. After determining the threat level that security plans must address, the NRC regulations specify the types of plant equipment that require protection and the level of protection required. For nuclear power plants, 10CFR73.55 specifies general performance objectives and requirements for the plant's physical security organization, physical barriers, access, detection, and communications.

This approach is similar to other NRC actions, such as regulations dealing with the spectrum of loss of coolant accidents (LOCAs) that emergency core cooling systems must be capable of mitigating. None of the sabotage regulations require quantitative analyses such as risk curves as a basis for acceptance. However, probabilistic techniques have played an important role in the NRC reviews of licensee security programs.

The NRC has used fault tree models as one tool for assessing the effectiveness of security programs. Fault tree models for almost every plant in the United

States have been prepared by the NRC. The models differ from typical PRA models by virtue of the fact that the vital equipment locations are included in the models. In a PRA, the fault tree models are reduced by computer algorithms to produce minimal cut sets. This qualitative analysis is necessary before data distributions can be propagated to produce a distribution for the system failure probability that eventually is part of the input to the risk curve (CCDF). For evaluating security programs, the location information included in the models is used to produce minimal cut sets containing location information instead of the actual vital equipment.

In addition, the fault tree models provide qualitative results that show the minimum number of areas that must be protected to ensure that the plant can be brought to a hot shutdown condition. This kind of qualitative information provides the NRC with a list of areas that can provide for safe plant shutdown in the event of a specific sabotage scenario.

EPA Approach to Human Intrusion

In contrast to the NRC, the EPA has chosen to include human intrusion (HI) in the quantitative analysis of performance assessment. In fact, the EPA not only requires that HI be considered, but also specifies how HI affects are to be calculated.

The EPA specifies a drilling density assumed to occur over a 10,000 year period. Further, the EPA allows no credit for active institutional controls beyond 100 years after repository closure. The EPA also states that passive institutional controls cannot be assumed to be a successful deterrent to a potential intruder.

To date, several attempts at developing and applying performance assessment methodologies to potential repository systems have been made[7,8,9]. In each case, the HI scenario has dominated the CCDF. In each case where the CCDF curves intersected the EPA requirements of part 191.13, removal of HI from the CCDF would eliminate the conflict. Figures 2 and 3 show CCDFs from studies along with the impact of HI on the numerical results.

COMMENTARY

Probabilistic techniques can be important tools in the regulatory arena. The products of probabilistic techniques can either be qualitative or quantitative in nature. The ability to use quantitative probabilistic techniques is highly dependent on the availability of data, the uncertainties in the data, and the uncertainties in the processes.

The dearth of data relating to sabotage events along with the uncertainties associated with the range of potential sabotage events and their impacts on engineered features led the NRC to chose a deterministic method for regulating licensee actions relating to physical plant protection in 10 CFR 73.55. The NRC uses qualitative probabilistic techniques as one measure of the effectiveness of licensee programs.

The EPA has decided to require development of a quantitative probabilistic

analysis in the form of a risk curve covering repository performance over a 10,000 year period as the basis for licensing a geologic HLW repository. Treatment of human intrusion is required as part of this analysis and the EPA standards specify that it must be included quantitatively. Whether this analysis should be quantitative, however, appears to be in question. Reasons for excluding human intrusion from the quantitative analysis follow.

Current PRA techniques have considerable difficulty quantifying human actions. The actions that PRAs try to include are those where operators fail to follow required actions (typically known as acts of omission). Acts of commission (such as sabotage or actions that operators might take that bypass engineered features when there is no compelling reason to take the action at all) are routinely excluded from quantitative risk assessments for nuclear power plants. The reason is simple. No one has produced a reliable method for predicting either the frequency or the effects of such actions. Qualitative methods using probabilistic techniques exist (such as confusion matrices and other tools) that can help to identify potential interactions, but none of these claim to be comprehensive even in the qualitative sense. Analyzing acts of commission over a 10,000 year time frame as required in the case of a geologic HLW repository would be even more difficult.

Except human intrusion, the EPA guidelines in 40CFR191 do not specify either the frequency of the scenarios that could adversely affect the protective features nor do they specify the ability of these features to withstand the potential scenario. Rather, the EPA requires that the analyses provide "reasonable expectation, based on performance assessments that the cumulative releases of radionuclides to the accessible environment for 10,000 years after disposal from all significant processes and events.." have less than a one in ten chance of exceeding the values in Table 1 of the rule and less than a one chance in 1,000 of exceeding ten times the Table 1 values.

For human intrusion, the EPA provides guidance on the frequency of the event, disallows any consideration of active institutional controls, and declares that passive controls can never be used to eliminate HI from consideration. This appears to be different from the other parts of the analyses that make up the quantitative risk curve. Limited performance assessment activities to date have indicated that the prescribed method of analyzing HI leads to CCDFs that exceed the EPA requirements.

The EPA regulations do not address the potential impact of human intrusion for alternate means of disposal compared to the deep geological HLW repository. HLW already exists and the only method currently approved for storing HLW is spent fuel pools or dry cask storage. Potential human intrusion leading to releases from these storage facilities over a 10,000 year period (or from some other means of disposal not addressed by the regulations) might be greater than that allowed for a deep geological repository.

CONCLUSIONS

Human actions have the potential to adversely affect the protective systems that limit the release of radioactive material to the environment. The NRC and EPA have chosen vastly different ways to deal with such actions in their regulations

for nuclear power plants and HLW repositories.

The EPA has opted for a quantitative, probabilistic analysis that includes human intrusion as one of its parts. The EPA guidelines specify the frequency of the HI events and the effectiveness of controls to prevent intrusion for the analysis. No such specification of frequencies or effectiveness of engineered systems for other scenarios is stipulated.

The NRC has opted for a deterministic approach for plant security. In a method similar to their treatment of design basis events, the NRC has specified a threat level that security plans must account for. The NRC requires identification of vital equipment and the areas encompassing vital equipment. Probabilistic techniques are used internally by the NRC staff to produce qualitative results that support the evaluation of the effectiveness of licensee security programs. Quantitative risk curves are not a licensing requirement for this issue. In fact, the NRC does not have any licensing criteria that require a risk curve comparison to a numerical standard.

This paper addresses the methods that the NRC and the EPA use to regulate protection from sabotage at reactors and inadvertent human intrusion at a potential HLW repository. While there may be concerns regarding the similarity of the events themselves (and therefore the applicability of comparing the types of regulation) and whether either agency has come upon the ultimate methodology for regulating them, this paper compares the regulations and applications as they currently exist. It is for the reader to determine the applicability of these techniques to the regulation of protection against sabotage at reactors and human intrusion at a HLW repository.

REFERENCES

1. Code of Federal Regulations, Title 10, Part 73, Physical Protection of Plants and Materials.

2. Code of Federal Regulations, Title 40, Part 191, Environmental Standards for the Management and Disposal of Spent Nuclear Fuel, High-Level and Transuranic Radioactive Wastes.

3. NUREG/CR-2300, PRA Procedures Guide.

4. NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.

5. NUREG-0800, Standard Review Plan, Chapter 13.6 Physical Security.

6. USNRC Review Guideline 17, Definition of Vital Areas and Equipment.

7. NUREG/CR-4510 (SAND86-0121), Assessing Compliance With the EPA High-Level Waste Standard: An Overview.

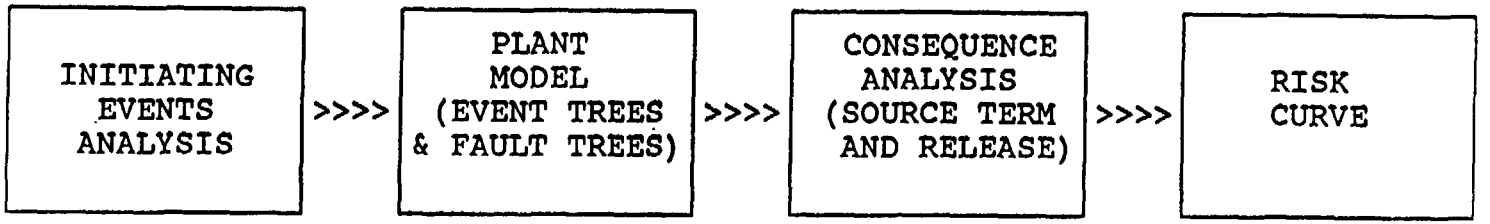
8. SANDIA presentation, 25th ACNW meeting transcript, October 24, 1990.

9. NRC staff presentation, 25th ACNW meeting transcript, October 25, 1990.

10. GAO Report to Congress, Security at Nuclear Power Plants- At Best, Inadequate, April 7, 1977.

11. GAO Report to NRC Chairman, Additional Improvements Needed in Physical Security at Nuclear Power Plants, July 13, 1983.

PROBABILISTIC RISK ASSESSMENT ELEMENTS



PERFORMANCE ASSESSMENT ELEMENTS

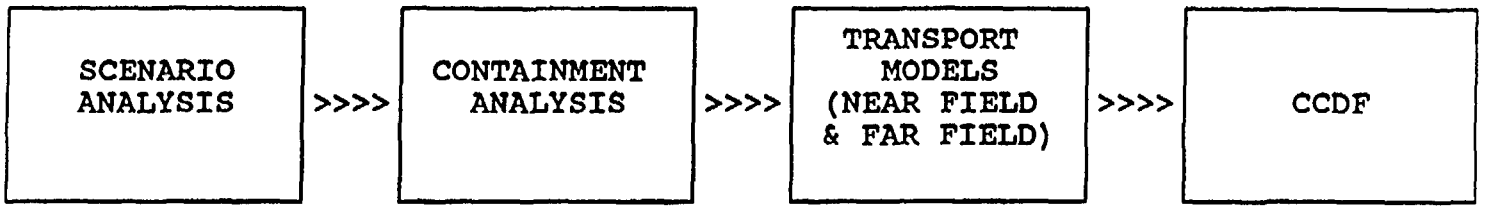
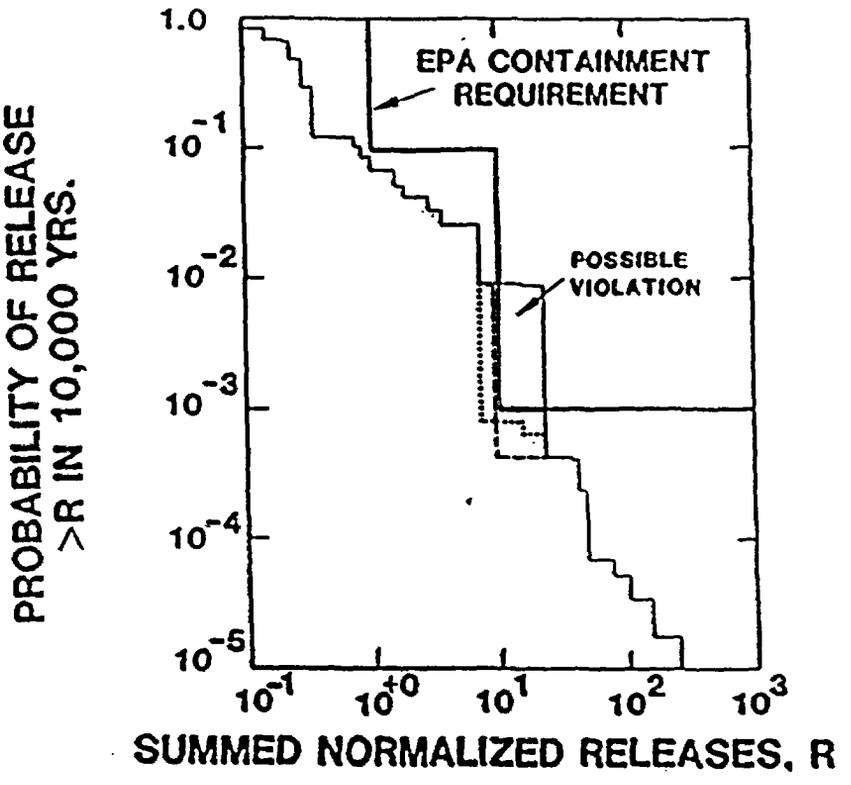
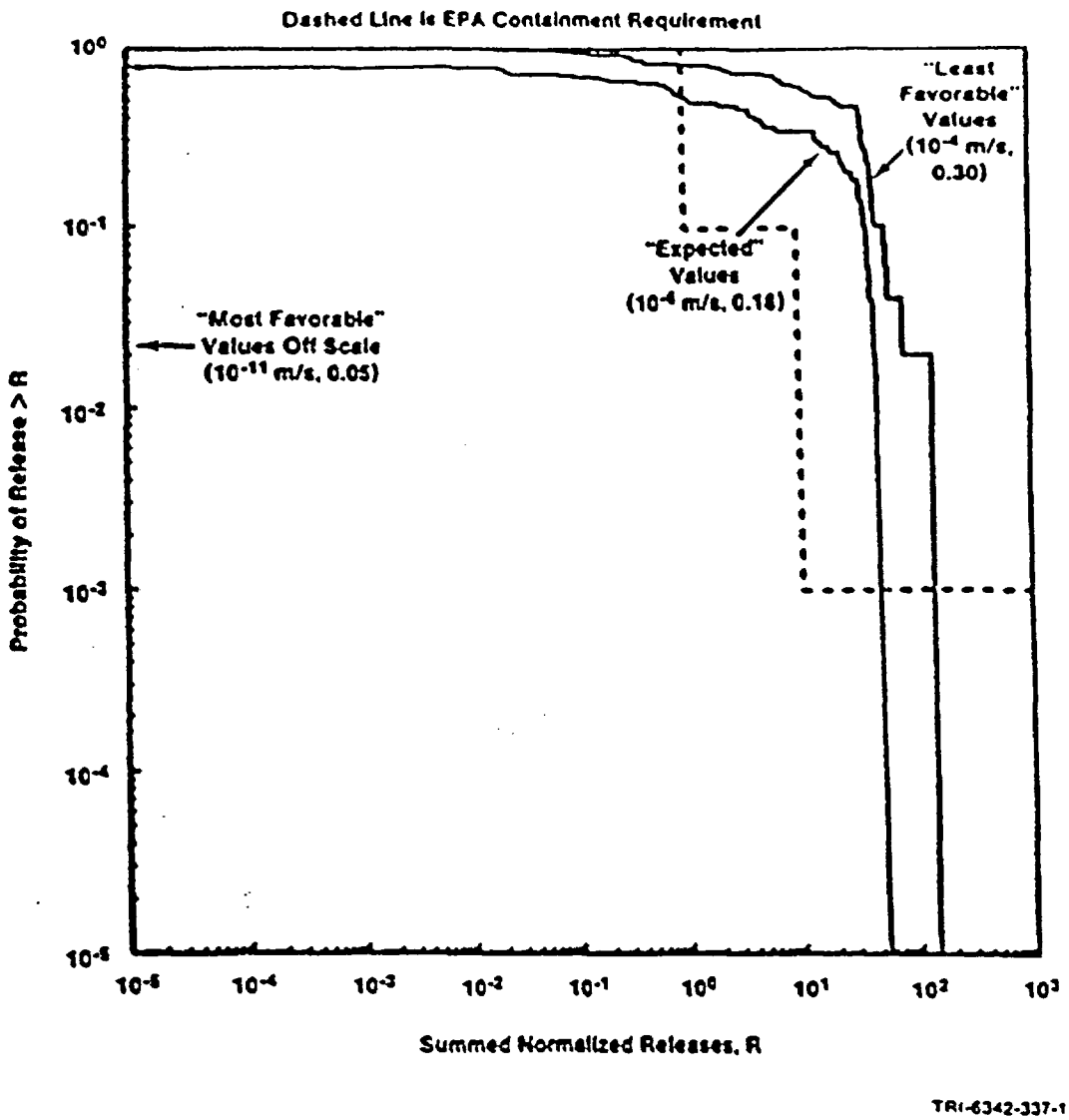


Figure 1. Comparison of PRA and PA Elements



CCDF for the Example plotted with EPA containment requirement.

Figure 3. SANDIA Report SAND86-0121-(NUREG/CR-4510) Overview of Assessing Compliance with 10 CFR 191



Conditional CCDF curves showing sensitivity to variations in borehole-plug porosity and hydraulic conductivity (Anderson et al., 1990). "Expected" and "least favorable" values for deteriorated borehole-plug porosity and hydraulic conductivity are shown. "Most favorable" values, corresponding to the properties of the repository seals, plot off-scale. Curves assume intrusion scenario E1 occurs. Curves were calculated using the preliminary modeling system described in Marietta et al. (1989) and cannot be used to judge compliance or noncompliance because all significant scenarios are not included, crucial models and data are missing, surface releases are omitted, and the Standard has been vacated. They simply measure modeling sensitivity to variations in the test parameters.

Figure 2. SANDIA Analysis of WIPP Performance for Human Intrusion